

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications)	CC Docket No. 96-115
Act of 1996:)	
)	
Telecommunications Carriers' Use of)	
Customer Proprietary Network Information)	
and other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security)	RM-11277
and Authentication Standards for Access to)	
Customer Proprietary Network Information)	

COMMENTS OF CROWN CASTLE INTERNATIONAL CORP.

Pursuant to §1.419 of the Commission's Rules, Crown Castle International Corp. ("Crown Castle") hereby submits its comments in the above-captioned proceeding.

I. INTRODUCTION

Crown Castle is primarily engaged in the business of owning, managing, and leasing to wireless network operators communications towers and similar infrastructure, with over 10,000 sites across the United States. Among its ancillary operations, Crown Castle subsidiaries own and operate several small land mobile radio systems, including a multi-site trunked 800 MHz specialized mobile radio ("SMR") system licensed to Crown Castle International Corp. de Puerto Rico ("CCPR"), and conventional UHF systems in Pennsylvania licensed to Crown Castle USA Inc. and Crown Communication Inc. CCPR and Crown Communication Inc. also operate common carrier microwave networks in Puerto Rico and Pennsylvania, respectively.

As an adjunct to its tower operations, Crown Castle develops, owns and operates shared, neutral-host distributed antenna systems (“DAS”) leased to FCC-licensed cellular, ESMR and PCS carriers, and operates as a regulated competitive local exchange carrier (“CLEC”) in several states.¹ These DAS systems include the construction and operation of active fiber-optic distribution networks which relay RF signals between remote antennas and central base-station transceiver (“BTS”) facilities of the wireless carriers.

As such, Crown Castle operates several “networks,” as that term is defined in the Communications Act. As a network operator, Crown Castle is concerned that the revisions proposed by the Electronic Privacy Information Center (“EPIC”) are overly complicated and create a significant administrative burden for Crown Castle and similarly situated network operators. Crown Castle respects the need for customer privacy and understands the recent Congressional and Commission concerns about the privacy of individual call records held by cellular and PCS providers. However, Crown Castle and other specialized CLEC and private mobile radio service (“PMRS”) operators are unintended victims in EPIC’s broad-brush solution, and need appropriate relief to balance privacy rules with the nature of the threat.

II. DISCUSSION

1. The Commission should create a Customer Proprietary Network Information (“CPNI”) “Safe Harbor” for PMRS operators

Like many “traditional” SMR operators, Crown Castle operates high-site analog trunked radio networks providing unlimited service to customers who pay a flat monthly fee. The overwhelming majority of SMR customers are business users who place a greater value on efficiency over privacy. Short of the identity of its customers and the number of units each

¹ Crown Castle’s wholly-owned subsidiaries include CLECs registered in seven states and the District of Columbia.

operates, non-interconnected SMRs collect and maintain little in the way of CPNI. Typically, this information is used only for billing and record-keeping, is not used by the SMR operator to market different classes of services, and is not sold, leased or loaned to third parties for their own marketing efforts. The Commission's current rules strike an appropriate balance between customer privacy and business efficiency by allowing a simple compliance mechanism for small PRMS operators like Crown Castle. Such network operators can avoid the complexity of establishing a customer approval system required by §64.2007² by simply abstaining from all uses of CPNI except those permitted by §64.2005.³

By contrast, the additional requirements sought to be imposed by EPIC would place burdensome requirements on every network operator and its customers in the name of preventing the already-illegal abuses of a few individuals who have obtained cellular call detail records ("CDR") through pretexting or outright theft. Proposed requirements such as customer-set passwords, audit trails tracking every single point of access to CPNI, and data encryption will create overwhelming burdens on Crown Castle and its customers, all in an effort to protect information which is simply not sensitive to the very customers to whom the privilege of protection purportedly flows. The burdens of compliance will frustrate customers, and overwhelm operators who may only earn a few thousand dollars in annual system revenue.

If the Commission feels the need to tighten restrictions on the handling and use of CPNI by large commercial mobile radio service ("CMRS") network operators, it should create a "safe harbor" allowing PMRS operators to receive a blanket exemption from the rules by certifying: (1) the network operator does not collect any CDR information; (2) the network operator does not use CPNI for any purpose other than as set forth in 47 C.F.R. §64.2005; and (3) the network

² 47 C.F.R. §64.2007.

³ 47 C.F.R. §64.2005.

operator does not disclose CPNI to third parties except as specifically permitted in 47 C.F.R. §64.2005. This safe harbor provision still provides the CPNI protections mandated within the framework of §222 of the Telecommunications Act, while mitigating the unintended effects of heightened CMRS privacy requirements which the Commission may choose to implement as part of this rulemaking.

2. The Commission should create a CPNI exception for wholesale-only networks

As with non-interconnected SMR operations, Crown Castle and similarly situated distributed antenna system operators will be unintended victims of the CPNI rule changes proposed by EPIC. Crown Castle constructs and operates specialized fiber optic networks for the single purpose of connecting shared wireless antennas (known as remote access nodes (“RANs”) and typically mounted on utility poles) with wireless-carrier specific BTS equipment which controls the transmission and reception of the carrier’s RF signal through the RANs. Each DAS network serves a fixed number of carrier customers, as determined by the frequency “cards” which can be held simultaneously by any single RAN. For the cellular, PCS and ESMR carriers who contract with Crown Castle to use the DAS network, the system provides extended or enhanced coverage, and is offered to all subscribers as an undifferentiated part of the carrier’s network coverage.

These DAS networks are becoming an increasingly common alternative to provide wireless coverage in hard-to-reach indoor and outdoor environments, with neutral-host solutions constructed and operated by Crown Castle and several competitors.⁴ Although Crown Castle entities are registered CLECs in several states to allow for utility pole attachments and right-of-way access, Crown Castle provides no retail or customer services, does not connect to the public

⁴ Crown Castle competes with other DAS network operators including NextG Networks, Clearlinx, InSite Wireless, Concourse, and American Tower.

telephone switched network, does not market dark fiber capacity, and does not sell any services except for integrated carrier use of the entire DAS system.

In the operation of DAS networks, Crown Castle does possess “information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier,”⁵ but such information is limited, and falls within two categories: (1) publicly available information (such as the location of network facilities and frequencies licensed to each carrier), and (2) private information which is protected by non-disclosure agreements between Crown Castle and each of its customers.

In this limited, specialized wholesale forum, the parties may take adequate steps through private contract to protect any information each customer considers to be proprietary. Since the wholesale issue is addressed neither by the EPIC petition nor the NPRM, this is obviously not an area of concern. Therefore, to the extent that any changes to Commission rules under this proceeding add greater procedural requirements to the protection of CPNI, those enhanced safeguards should contain appropriate exceptions to avoid placing undue burden on Crown Castle and other operators of purely wholesale DAS networks.

III. CONCLUSION

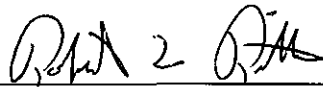
In crafting changes to its CPNI rules, the Commission should provide reasonable flexibility so that PMRS operators and wholesale CLECs are not irrationally overwhelmed with a one-size-fits-all approach. The privacy of business customers buying system capacity is just not the problem to be solved in this proceeding. If the Commission adopts the proposals from the EPIC petition, Crown Castle and similarly situated network operators will be innocent victims

⁵ 47 U.S.C. §222(h)(1)(A).

whose competitive ability is hampered by, in racing parlance, being "caught up in somebody else's mess." For these reasons, we respectfully request that the Commission weigh these interests and create appropriate application of the rules to these specialized networks.

Respectfully submitted,

CROWN CASTLE INTERNATIONAL CORP.

By:  _____

Robert L. Ritter, Attorney
Monica Gambino, Vice President, Legal

2000 Corporate Drive
Canonsburg, PA 15317
Phone: (724) 416-2000
Fax: (724) 416-2353

April 13, 2006

CERTIFICATE OF SERVICE

I, Robert L. Ritter, an attorney at Crown Castle International Corp., do hereby certify that I have on this 13th day of April, 2006, sent via First Class, United States Mail, postage prepaid, a copy of the foregoing Comments to the following:

Chris Jay Hoofnagle, Senior Counsel
Electronic Privacy Information Center
West Coast Office
944 Market Street, Suite 709
San Francisco, CA 94102

By:  _____
Robert L. Ritter